The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
1/15/2010

SUBJECT:
Vulnerability in Internet Explorer Could Allow Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. **At this point in time, no patches are available for this vulnerability**. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of this vulnerability. Successful exploitation of the vulnerability could allow an attacker to gain the same user rights as the local user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed attacks may cause denial-of-service conditions.

Microsoft is reporting that this vulnerability is being actively exploited on the Internet.

SYSTEMS AFFECTED:

Microsoft Internet Explorer 6
Microsoft Internet Explorer 7
Microsoft Internet Explorer 8

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability exists in the way Internet Explorer accesses an object that has been deleted. Once deleted, this vulnerability will allow access to an invalid pointer object. An attacker could exploit this vulnerability by constructing a specially crafted web page. When a user views the web page, the vulnerability could allow for remote code execution.

Successful exploitation of the vulnerability could allow an attacker to gain the same user rights as the local user. Depending on the privileges associated with the user, the attacker could then install programs; view, change, or delete data; or create new accounts with full privileges. **At this point in time, no patches are available for this vulnerability**.

Microsoft is reporting that this vulnerability is being actively exploited on the Internet.

RECOMMENDATIONS:
The following actions should be taken:

Consider applying appropriate workarounds recommended by Microsoft to vulnerable systems immediately after appropriate testing:

- Set Internet and Local intranet security zone settings to "High" to prompt before running ActiveX Controls and Active Scripting in these zones
- Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone
- Enable DEP for Internet Explorer 6 Service Pack 2 or Internet Explorer 7
- Consider using an alternate web browser until a patch is available.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Ensure that all anti-virus software is up to date with the latest signatures.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.
- If you believe you have been affected by attacks exploiting this vulnerability, please contact us immediately.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/advisory/979352.mspx
http://blogs.technet.com/msrc/archive/2010/01/14/security-advisory-979352.aspx

Secunia:
http://secunia.com/advisories/38209/

US-CERT:
http://www.kb.cert.org/vuls/id/492515

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0249

Vupen:
http://www.vupen.com/english/advisories/2010/0135

Security Focus:
http://www.securityfocus.com/bid/37815